DATA AUTHENTICATION SYSTEM EMPLOYING ENCRYPTED INTEGRITY BLOCKS

FIELD OF INVENTION

This application is a continuation-in-part of 09/250935, filed February 18, 1999. ABN

The invention relates generally to data communications networks and, in particular, to systems for authentication of data transferred over the networks.

BACKGROUND OF THE INVENTION

When a sender transfers data over a network, an interloper may intercept and alter the data and then transfer the altered data to the intended recipients. The recipients, who presume the data are valid because they appear to come from a trusted sender, may then use the altered data directly, or introduce errors into associated data processing systems. To ensure that the received data were not altered enroute by an interloper, the network may include a data authentication system that essentially encodes the data at the sender and decodes the data at the recipient to detect changes in the data.

One known data authentication process involves including a digital signature in a data packet. The digital signature is produced by first encoding the packet data bytes to produce a cryptographic hash and then, typically, encrypting the hash using the sender's private key. A recipient uses the sender's public key to decrypt the digital signature and reproduce the hash. It then encodes the received data using the same cryptographic hash function and compares the result with the decrypted hash. If the two hashes match, the data is considered authentic, that is, the received data is considered to be the same data that was sent by the sender who holds the private key. This authentication process works well, but it is both computation intensive and time consuming at the recipient end.